

JOSEPH W. PRICE
ALBIN H. GESS
MICHAEL J. MOFFATT
GORDON E. GRAY III
BRADLEY D. BLANCHE

e-mail: pgu@pgulaw.com



PRIORITY DOCUMENT
(Japan 2000-381870)

Inventor(s): Yukiyasu Fukami

Title: BROADCAST APPARATUS AND RECEPTION APPARATUS FOR PROVIDING A STORAGE SERVICE BY WHICH SCRAMBLED CONTENT IS STORED AND DESCRAMBLLED USING SCRAMBLING KEY LIST

Attorney's
Docket No.: NAK1-BQ58

EXPRESS MAIL LABEL NO. EL 873069417 US

DATE OF DEPOSIT: December 13, 2001

JWPRI 447/261-8455

NEKJ DQ08
Yukiyasu Fukumiet al,

10858 U.S. PTO
10/023021
12/13/01

日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出 願 年 月 日
Date of Application:

2000年12月15日

出 願 番 号
Application Number:

特願2000-381870

出 願 人
Applicant(s):

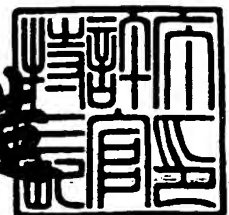
松下電器産業株式会社

CERTIFIED COPY OF
PRIORITY DOCUMENT

2001年 9月13日

特 許 庁 長 官
Commissioner,
Japan Patent Office

及 川 耕 造



出証番号 出証特2001-3084745

【書類名】 特許願

【整理番号】 2022520548

【提出日】 平成12年12月15日

【あて先】 特許庁長官殿

【国際特許分類】 H04N 7/16

【発明者】

【住所又は居所】 愛知県名古屋市中区栄2丁目6番1号白川ビル別館5階
株式会社松下電器情報システム名古屋研究所内

【氏名】 深見 幸靖

【発明者】

【住所又は居所】 大阪府門真市大字門真1006番地 松下電器産業株式
会社内

【氏名】 中原 徹

【発明者】

【住所又は居所】 大阪府門真市大字門真1006番地 松下電器産業株式
会社内

【氏名】 松尾 隆史

【発明者】

【住所又は居所】 大阪府門真市大字門真1006番地 松下電器産業株式
会社内

【氏名】 東 吾紀男

【発明者】

【住所又は居所】 大阪府門真市大字門真1006番地 松下電器産業株式
会社内

【氏名】 村上 弘規

【特許出願人】

【識別番号】 000005821

【氏名又は名称】 松下電器産業株式会社

【代理人】

【識別番号】 100097445

【弁理士】

【氏名又は名称】 岩橋 文雄

【選任した代理人】

【識別番号】 100103355

【弁理士】

【氏名又は名称】 坂口 智康

【選任した代理人】

【識別番号】 100109667

【弁理士】

【氏名又は名称】 内藤 浩樹

【手数料の表示】

【予納台帳番号】 011305

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9809938

【書類名】 明細書

【発明の名称】 限定受信方法およびシステム

【特許請求の範囲】

【請求項 1】 有料番組を配信する放送装置と、前記有料番組を受信して再生する受信装置から構成される限定受信システムであって、

放送装置は、

スクランブル鍵を取得するスクランブル鍵取得手段と、

前記スクランブル鍵からスクランブル鍵リストを作成するスクランブル鍵リスト生成手段と、

前記スクランブル鍵リストを含む蓄積用 E C M を作成する E C M 生成手段と、

前記蓄積用 E C M を周期的に送出する E C M 送出手段と、

前記スクランブル鍵リストからスクランブル鍵を抽出するスクランブル鍵リスト解釈手段と、

抽出した前記スクランブル鍵を用いてコンテンツをスクランブルするスクランブル処理手段と、

前記 E C M 送出手段から送出された蓄積用 E C M と、スクランブルされた前記コンテンツを多重化して有料番組を配信する多重化処理手段を備え、

受信装置は、

受信した有料番組から蓄積用 E C M とスクランブルされたスクランブルコンテンツを分離する分離手段と、

分離した前記蓄積用 E C M と前記スクランブルコンテンツを蓄積する蓄積手段と、

前記蓄積用 E C M からスクランブル鍵リストを抽出する E C M 解釈手段と、

前記スクランブル鍵リストからスクランブル鍵を抽出するスクランブル鍵リスト解釈手段と、

抽出した前記スクランブル鍵で前記スクランブルコンテンツをデスクランブルするデスクランブル処理手段と、

前記デスクランブルされたコンテンツを再生する再生処理手段を備えたことを特徴とする限定受信システム。

【請求項 2】 前記放送装置は、コンテンツを T S パケット化する T S パケット化処理手段と、

前記 T S パケットをひとつずつ取得し、取得した T S パケットが先頭から何番目かをカウントする T S パケットカウンタ手段をさらに備え、

前記スクランブル鍵リスト解釈手段は、前記 T S パケットのカウント値を基に前記スクランブル鍵リストからスクランブル鍵を抽出し、

一方、前記受信装置は、前記蓄積手段に蓄積されている前記スクランブルコンテンツからひとつずつ T S パケットを取り出し、取り出した T S パケットが先頭から何番目かを T S パケットインデックスとしてカウントする T S パケット抽出手段をさらに備え、

前記スクランブル鍵リスト解釈手段は、前記 T S パケットの T S パケットインデックス値を基に前記スクランブル鍵リストからスクランブル鍵を抽出することを特徴とする請求項 1 に記載の限定受信システム。

【請求項 3】 前記放送装置の前記 E C M 生成手段は、前記スクランブル鍵リストを E C M のデータ形式のうち、暗号化対象部分に埋め込んで蓄積用 E C M を作成することを特徴とする請求項 1 に記載の限定受信システム。

【請求項 4】 前記放送装置の前記 E C M 生成手段は、従来の E C M と蓄積用 E C M を区別する情報を埋め込んだ形式で蓄積用 E C M を作成することを特徴とする請求項 1 に記載の限定受信システム。

【請求項 5】 前記 E C M 送出手段は、前記蓄積用 E C M を 1 回だけ送出することを特徴とする請求項 1 に記載の限定受信システム。

【請求項 6】 前記放送装置は、コンテンツを T S パケット化する T S パケット化処理手段と、

前記 T S パケットの非スクランブルな特定の情報を取り出して解釈する T S パケットヘッダ解釈手段をさらに備え、

前記スクランブル鍵リスト解釈手段は、前記特定の情報を基に前記スクランブル鍵リストからスクランブル鍵を抽出し、

一方、前記受信装置は、前記蓄積手段に蓄積されている前記スクランブルコンテンツからひとつずつ T S パケットを取り出し、前記 T S パケットの非スクラン

ブルな特定の情報を取り出すTSパケット抽出手段をさらに備え、

前記スクランブル鍵リスト解釈手段は、前記特定の情報を基に前記スクランブル鍵リストからスクランブル鍵を抽出する

ことを特徴とする請求項1に記載の限定受信システム。

【請求項7】 前記放送装置は、前記特定の情報に対して演算を行うスクランブル鍵識別子算出手段をさらに備え、

前記スクランブル鍵リスト解釈手段は、演算された前記特定の情報を基に前記スクランブル鍵リストからスクランブル鍵を抽出し、

一方、前記受信装置は、前記特定の情報に対して演算を行うスクランブル鍵識別子算出手段をさらに備え、

前記スクランブル鍵リスト解釈手段は、演算された前記特定の情報を基に前記スクランブル鍵リストからスクランブル鍵を抽出する

ことを特徴とする請求項6に記載の限定受信システム。

【請求項8】 受信した有料番組から蓄積用ECMとスクランブルされたスクランブルコンテンツを分離する分離手段と、

分離した前記蓄積用ECMと前記スクランブルコンテンツを蓄積する蓄積手段と、

前記蓄積用ECMからスクランブル鍵リストを抽出するECM解釈手段と、

前記蓄積手段に蓄積されている前記スクランブルコンテンツからひとつずつTSパケットを取り出し、取り出したTSパケットが先頭から何番目かをTSパケットインデックスとしてカウントするTSパケット抽出手段と、

前記TSパケットのTSパケットインデックス値を基に前記スクランブル鍵リストからスクランブル鍵を抽出するスクランブル鍵リスト解釈手段と、

抽出した前記スクランブル鍵で前記スクランブルコンテンツをデスクランブルするデスクランブル処理手段と、

前記デスクランブルされたコンテンツを再生する再生処理手段を備えたことを特徴とする受信装置。

【請求項9】 前記TSパケット抽出手段は、ひとつのTSパケットを抽出する毎に、当該パケットがIピクチャであるか判断し、Iピクチャである場合にの

み前記TSパケットを前記デスクランブル処理手段へ送ることによって特殊再生を行うことを特徴とする請求項8に記載の受信装置。

【請求項10】 前記ECM解釈手段で抽出したスクランブル鍵リストを保持するスクランブル鍵リスト保持手段と、前記スクランブル鍵リスト解釈手段をセキュリティモジュール内部に備えることを特徴とする請求項8に記載の受信装置。

【請求項11】 有料番組を配信する放送装置と、前記有料番組を受信して再生する受信装置から構成される限定受信方法であって、

放送装置は、

スクランブル鍵を取得するスクランブル鍵取得ステップと、

前記スクランブル鍵からスクランブル鍵リストを作成するスクランブル鍵リスト生成ステップと、

前記スクランブル鍵リストを含む蓄積用ECMを作成するECM生成ステップと、

前記蓄積用ECMを周期的に送出するECM送出ステップと、

前記スクランブル鍵リストからスクランブル鍵を抽出するスクランブル鍵リスト解釈ステップと、

抽出した前記スクランブル鍵を用いてコンテンツをスクランブルするスクランブル処理ステップと、

前記ECM送出手段から送出された蓄積用ECMと、スクランブルされた前記コンテンツを多重化して有料番組を配信する多重化処理ステップを備え、

受信装置は、

受信した有料番組から蓄積用ECMとスクランブルされたスクランブルコンテンツを分離する分離ステップと、

分離した前記蓄積用ECMと前記スクランブルコンテンツを蓄積する蓄積ステップと、

前記蓄積用ECMからスクランブル鍵リストを抽出するECM解釈ステップと

前記スクランブル鍵リストからスクランブル鍵を抽出するスクランブル鍵リスト解釈ステップと、

抽出した前記スクランブル鍵で前記スクランブルコンテンツをデスクランブルするデスクランブル処理ステップと、

前記デスクランブルされたコンテンツを再生する再生処理ステップを備えたことを特徴とする限定受信方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、デジタル放送における限定受信方法およびシステムに関し、特に、蓄積型サービスにおける有料番組のスクランブル鍵送出方法に関する。

【0002】

【従来の技術】

現在のBSデジタル放送のCA (Conditional Access) 方式では、ECMに現在と次のスクランブル鍵を記述して送出される。また、チャンネル切替時に、映像および音声が出力されるまでの時間を短縮するなどの改良をした発明 (特開平11-340966) がある。

【0003】

【発明が解決しようとする課題】

しかしながら、コンテンツをHDDなどに蓄積した後で、コンテンツを視聴または購入する蓄積型サービスの開始が予定されている。その際にスクランブルコンテンツを蓄積後に特殊再生 (早送り再生、巻き戻し再生など) やランダムアクセス (コンテンツの任意の場所から再生) を行う場合、従来の方式によると、視聴対象となる部分に対応するスクランブル鍵すなわちECM (Entitlement Control Message: 共通情報) を、蓄積したTS (Transport Stream) の中から検出し、スクランブル鍵を抽出した後でデスクランブル処理を行う必要がある。そのために、例えば早送り再生機能の性能が、十分ユーザの満足できるスピードにならない可能性がある。

【0004】

本発明は、スクランブルコンテンツを蓄積し、蓄積後の特殊再生機能を、ユーザの満足できる性能で実現することを目的とする。

【 0 0 0 5 】

【課題を解決するための手段】

この課題を解決するために本発明は、有料番組を配信する放送装置と、前記有料番組を受信して再生する受信装置から構成される限定受信システムであって、放送装置は、スクランブル鍵を取得するスクランブル鍵取得手段と、前記スクランブル鍵からスクランブル鍵リストを作成するスクランブル鍵リスト生成手段と、前記スクランブル鍵リストを含む蓄積用 E C M を作成する E C M 生成手段と、前記蓄積用 E C M を周期的に送出する E C M 送出手段と、前記スクランブル鍵リストからスクランブル鍵を抽出するスクランブル鍵リスト解釈手段と、抽出した前記スクランブル鍵を用いてコンテンツをスクランブルするスクランブル処理手段と、前記 E C M 送出手段から送出された蓄積用 E C M と、スクランブルされた前記コンテンツを多重化して有料番組を配信する多重化処理手段を備え、一方、受信装置は、受信した有料番組から蓄積用 E C M とスクランブルされたスクランブルコンテンツを分離する分離手段と、分離した前記蓄積用 E C M と前記スクランブルコンテンツを蓄積する蓄積手段と、前記蓄積用 E C M からスクランブル鍵リストを抽出する E C M 解釈手段と、前記スクランブル鍵リストからスクランブル鍵を抽出するスクランブル鍵リスト解釈手段と、抽出した前記スクランブル鍵で前記スクランブルコンテンツをデスクランブルするデスクランブル処理手段と、前記デスクランブルされたコンテンツを再生する再生処理手段を備えたことを特徴とする。

【 0 0 0 6 】

【発明の実施の形態】

以下、本発明の実施の形態について図面を用いて説明する。

【 0 0 0 7 】

(実施の形態 1)

図 1 は、本発明の実施の形態 1 によるシステム全体の構成を示す図である。システムは放送装置 1 0 0 と、受信機 2 0 0 とセキュリティモジュール 3 0 0 から

構成されている。なお、セキュリティモジュール 3 0 0 は、物理的には通常 I C カードとして実現され、受信機 2 0 0 にセットして使用される。放送装置 1 0 0 は、T S パケット化処理部 1 0 1 と、スクランブル鍵リスト生成部 1 0 2 と、スクランブル処理部 1 0 3 と、E C M 生成部 1 0 4 と、E C M 送出部 1 0 5 と、多重化処理部 1 0 6 と、コンテンツ取得部 1 0 7 と、スクランブル鍵取得部 1 0 8 とから構成されている。受信機 2 0 0 は、T S 分離部 2 0 1 と、蓄積装置である HDD 2 0 2 と、スクランブル鍵リスト保持部 2 0 3 と、デスクランブル処理部 2 0 4 と、再生処理部 2 0 5 とから構成されている。セキュリティモジュール 3 0 0 は、E C M 解釈部 3 0 1 から構成されている。

【 0 0 0 8 】

図 2 は放送装置 1 0 0 のスクランブル処理部 1 0 3 の構成をさらに詳しく示した図である。スクランブル処理部 1 0 3 は、T S パケットカウンタ部 1 1 0 と、スクランブル鍵リスト保持部 1 1 1 と、スクランブル部 1 1 2 と、スクランブル鍵リスト解釈部 1 1 3 からなる。

【 0 0 0 9 】

なお、図 1、図 2 では現行 B S デジタル放送システムとの違いを明記するために、蓄積用 E C M を作成して送出する系とは異なる現行 B S デジタル放送システムにおける E C M を作成して送出する系も併記しており、スクランブル鍵取得部 1 0 8 で取得したスクランブル鍵をスクランブル処理部 1 0 3 および E C M 生成部 1 0 4 へ渡す部分が現行 B S デジタル放送システムでの系である（図中点線で示している）。

【 0 0 1 0 】

図 3 は受信機 2 0 0 のデスクランブル処理部 2 0 4 の構成をさらに詳しく示した図である。デスクランブル処理部 2 0 4 は、T S パケット抽出部 2 1 0 と、デスクランブル部 2 1 1 と、スクランブル鍵リスト解釈部 2 1 2 からなる。

【 0 0 1 1 】

次に T S パケットとスクランブルキーの対応（スクランブル鍵リストから該当 T S パケットのスクランブル鍵を抽出するための情報）を E C M（E n t i t l e m e n t C o n t r o l M e s s a g e：共通情報）に記述する方法につ

いて放送装置側における詳細な動作および、受信機側における詳細な動作について説明する。

【 0 0 1 2 】

(放送装置側)

図4は放送装置100において映像、音声、データなどのコンテンツにスクランブルをかける際の動作手順を示すフローチャートである。図1と図2も用いて説明する。まず、スクランブル鍵取得部108でスクランブル鍵を取得し、取得したスクランブル鍵をスクランブル鍵リスト生成部102へ渡す(ステップS501)。次に、スクランブル鍵リスト生成部102でスクランブル鍵リストを作成する(ステップS502)。スクランブル鍵リストの一例としては、図9にデータ構造を示すようなスクランブル鍵リスト記述子がある。スクランブル鍵リスト記述子は、スクランブル鍵の識別をするスクランブル鍵識別子(Ks__id)とスクランブル鍵(Ks)と当該KsでスクランブルするTSパケット数(TS__packet__number)から構成され、Ksの数分Ks__idとKsとTS__packet__numberとが記述される。次に、ECM生成部104において、図8にデータ構造を示すように、BSデジタル放送方式で規定されているECM本体の可変部(暗号化対象)に、上記スクランブル鍵リスト記述子を追加することによって、蓄積用ECMを作成し(ステップS503)、ECM送出部105から多重化処理部106へ送出する(ステップS504)。蓄積用ECMとは蓄積再生機能(蓄積したコンテンツをタイムシフト視聴できる機能)用を使用するECMであり、従来のECMと区別するための情報を埋め込む。上記ステップS503で、例えば、図8に示すように、セクションヘッダ部のテーブル識別子の値を、従来のECMと蓄積用ECMで異なる値にする。なお、テーブル識別子は同じ値にして、拡張テーブル識別子の値を異なる値にしてもよい。一方、コンテンツ取得部107で取得した映像、音声、データなどのコンテンツを、TSパケット化処理部101においてTSパケット化し(ステップS505)、スクランブル処理部103でスクランブルをかけ(ステップS506)、多重化処理部106においてスクランブルコンテンツと蓄積用ECMを多重化した(ステップS507)有料番組をTSとして放送する。本明細書ではスクランブル

コンテンツと蓄積用 ECM を多重化したものを有料番組と定義する。

【 0 0 1 3 】

なお、図 1 はスクランブル鍵、コンテンツを放送装置 1 0 0 とは別の装置で作成する前提で記述したが、スクランブル鍵、コンテンツともに放送装置 1 0 0 内で作成してもよいし、どちらか一方のみ放送装置 1 0 0 内で作成してもかまわない。

【 0 0 1 4 】

次に、図 5 にスクランブル処理部 1 0 3 の処理（図 4 ステップ S 5 0 6）の詳細フローチャートを示す。スクランブル鍵リスト生成部 1 0 2 から、スクランブル鍵リストを取得し、スクランブル鍵リスト保持部 1 1 1 に格納する（ステップ S 6 0 1）。TS パケット化処理部 1 0 1 に TS パケット化された（ステップ S 5 0 4）コンテンツを TS パケットカウンタ部 1 1 0 において、1 TS パケット分取得する（ステップ S 6 0 2）。1 TS パケット分取得した時に TS パケットカウンタ部 1 1 0 は、TS パケット数を累積することによって、当該 TS パケットが先頭から何番目のパケットかをカウントし、TS パケット累積数（先頭から何番目のパケットかの情報）をスクランブル鍵リスト解釈部 1 1 3 へ渡し、TS パケットをスクランブル部 1 1 2 へ渡す（ステップ S 6 0 3）。なお、TS パケット累積数は、別のコンテンツに対して図 4 のフローチャートに示す処理をする前にリセットしておく。次に、スクランブル鍵リスト解釈部 1 1 3 において、TS パケット累積数とスクランブル鍵リスト保持部 1 1 1 に格納してあるスクランブル鍵リストから該当スクランブル鍵を抽出して、スクランブル部 1 1 2 へ渡す（ステップ S 6 0 4）。スクランブル部 1 1 2 において、ステップ S 6 0 3 で取得した 1 TS パケット分を、ステップ S 6 0 4 で取得したスクランブル鍵でスクランブルをかけ、多重化処理部 1 0 6 へ渡し（ステップ S 6 0 5）、全 TS パケット分取得したかどうかを判定して（ステップ S 6 0 6）、取得完了していれば処理を終了し、そうでなければ、ステップ S 6 0 2 からの処理を繰り返す。

【 0 0 1 5 】

以下に図 1 0 に示すような、説明のため簡略した具体例を用いて、ステップ S 6 0 4 の詳細な説明を行う。図 1 0 の例ではスクランブルをかけたいコンテンツ

T S が 4 0 0 T S パケットから構成され、先頭から 1 0 0 パケット分単位で、スクランブル鍵を変更する例である。図 1 0 の例におけるスクランブル鍵リストの具体例を図 1 1 に示す。

【 0 0 1 6 】

図 1 0 において 2 番目のパケットである T S P 2 をスクランブルする際に、該当スクランブル鍵を抽出する時の処理を示す。2 番目の T S パケットなので T S パケット累積数は 2 であり、図 1 1 のスクランブル鍵リストによると、先頭から 1 0 0 番目までの T S パケットのスクランブル鍵は K s 1 であるため、T S P 2 の該当スクランブル鍵は K s 1 であり、K s 1 を抽出する。同様に T S P 1 0 0 までの該当スクランブル鍵は K s 1 である。T S P 1 0 1 になると、T S パケット累積数は 1 0 1 番目の T S パケットなので 1 0 1 であり、図 1 1 のスクランブル鍵リストによると、スクランブル鍵は K s 1 ではなく次の K s 2 である。

【 0 0 1 7 】

(スクランブル鍵リスト送出タイミング)

次に、スクランブル鍵リストの送出タイミングの説明をする。スクランブル鍵リストはスクランブルコンテンツに対して少なくとも一つ、蓄積すれば良いため図 1 9 に示すように、現行 B S デジタル方式における送出周期に比べて、長い周期（例えば 1 0 倍程度）で送出すればよい。また確実に蓄積される保証があれば、スクランブルコンテンツに対して 1 度だけ送出してもよい。

【 0 0 1 8 】

(受信機側)

図 6 は T S 分離部 2 0 1 で、テーブル識別子または拡張テーブル識別子の値によって、従来の E C M と区別することによって蓄積用 E C M とスクランブルコンテンツを分離して H D D 2 0 2 に蓄積後に、受信機 2 0 0 でスクランブルコンテンツをデスクランブルする際の動作手順を示すフローチャートである。図 1 と図 3 も用いて説明する。なお、蓄積用 E C M とスクランブルコンテンツを分離せずに、一時的に一つの T S として蓄積し、蓄積後に分離してもよい。

【 0 0 1 9 】

まず、H D D 2 0 2 に蓄積してある蓄積用 E C M をセキュリティモジュール 3

00内のECM解釈部301へ渡す（ステップS701）。ECM解釈部301で蓄積用ECMからスクランブル鍵リストを抽出する（ステップS702）。ECM解釈部301から取得したスクランブル鍵リストをスクランブル鍵リスト保持部203に格納する（ステップS703）。一方、HDD202に蓄積してあるスクランブルコンテンツをデスクランブル処理部204へ渡し（ステップS704）、デスクランブル処理部204でデスクランブルする（ステップS705）。

【0020】

図7にデスクランブル処理部204の処理（ステップS705）の詳細フローチャートを示す。ステップS704で渡されたスクランブルコンテンツをTSパケット抽出部210において、1TSパケット分抽出する（ステップS801）。1TSパケット分抽出した時にTSパケット抽出部210は、当該TSパケットが先頭から何番目のパケットかをカウントし、その情報（以下、TSパケットインデックスと記述）を、スクランブル鍵リスト解釈部212へ渡し、抽出したTSパケットをデスクランブル部211へ渡す（ステップS802）。スクランブル鍵リスト解釈部212において、TSパケットインデックスとスクランブル鍵リスト保持部203に格納してあるスクランブル鍵リストから該当スクランブル鍵を抽出して、デスクランブル部211へ渡す（ステップS803）。デスクランブル部211において、ステップS802で取得した1TSパケット分を、ステップS803で取得したスクランブル鍵でデスクランブルし、再生処理部へ渡す（ステップS804）。全TSパケット分取得したかどうかを判定して（ステップS805）、取得完了していれば処理を終了し、そうでなければ、ステップS801からの処理を繰り返す。

【0021】

（特殊再生する際の受信機の詳細な動作）

次に、蓄積後のスクランブルコンテンツを特殊再生する際の受信機の詳細な動作について説明する。ここでは、特殊再生の代表的機能である早送り再生機能について説明する。MPEG2符号化方式では、映像ストリームは図21に示すようにIピクチャ（フレーム内符号化画像）、Bピクチャ（双方向予測符号化画像

）、Pピクチャ（フレーム間順方向予測符号化画像）の三種類のピクチャから構成され、Iピクチャのみ単独で復号することが可能なため、早送り再生機能は、ピクチャのみを再生することで実現する。次に、図21で示す映像ストリームをTSに変換した模式図を図12に示す。図12では簡易的に、図21のIピクチャを、図12の斜線部分のTSパケットに変換したと仮定する。すなわち最初のIピクチャがTSP2～TSP5へ、二番目のIピクチャがTSP101からTSP104へ、三番目のIピクチャがTSP201～TSP204へ、四番目のIピクチャがTSP301～TSP304へ変換できたとする。

【0022】

以下、斜線部分のTSパケットをデスクランブルする際の受信機の動作手順を説明する。スクランブル鍵リストは図11に示す。フローチャートは前述の図6には変更がなく、デスクランブル処理部の処理に一部変更があるため、デスクランブル処理部の処理を図22に示し、図7も用いて説明する。まず、TSパケット抽出部210において、スクランブルコンテンツを1TSパケット分抽出し（ステップS1101）、特殊再生処理かどうか判定して（ステップS1102）、特殊再生処理であればステップS1103へ移り、特殊再生処理でなければステップS1104へ移る。次に、TSパケット抽出部210において抽出したパケットがIピクチャかどうか判定して（ステップS1103）、IピクチャであればステップS1104へ移り、Iピクチャでなければ、ステップS1101へ戻る。ステップS1104以降の処理は、図7のステップS802以降と同様なので、図12に示す具体例で説明する。例えばIピクチャであるTSP2を抽出した時は、二番目のパケットなのでステップS1104でTSパケットインデックスを2と算出する。次に、ステップS1105で、図11のスクランブル鍵リストから該当スクランブル鍵Ks1を抽出し、ステップS1106で、TSP2をスクランブル鍵Ks1でデスクランブルする。同様に、TSP3～TSP5をスクランブル鍵Ks1でデスクランブルし、TSP101～TSP104をスクランブル鍵Ks2で、TSP201～TSP204をスクランブル鍵Ks3で、TSP301～TSP304をスクランブル鍵Ks4でデスクランブルする。

【0023】

ステップ S 1 1 0 3 における I ピクチャかどうかを判定する方法は、例えば特開平 8 - 3 4 0 5 4 1 に記述があるように、TS パケットの非スクランブル部分に I ピクチャであることがわかるような情報を送出時に埋め込んでおき、その情報を見て判定する。

【 0 0 2 4 】

なお、巻き戻し再生機能は、TS パケットの抽出順序を早送り再生機能の時と逆にすることで実現可能である。また、ランダムアクセス機能は、抽出する TS パケットの開始位置が異なるだけで、それ以外は同様な処理で実現可能である。つまり、デスクランブル対象である任意の TS パケットに対するスクランブル鍵を、スクランブル鍵リストから抽出することによって種々の特殊再生等が実現できる。

【 0 0 2 5 】

（実施の形態 2）

実施の形態 1 では、受信機内のセキュリティが保証されることを前提として、スクランブル鍵リスト保持部 2 0 3 およびスクランブル鍵リスト解釈部 2 1 2 が受信機内にある構成で説明した。しかし、図 1 3 に示すように、スクランブル鍵リスト保持部 2 0 3 およびスクランブル鍵リスト解釈部 2 1 2 がセキュリティモジュール 3 0 0 内にあるような構成にすれば、スクランブル鍵リストの安全性を高めることができる。図 1 4 にデスクランブル処理部の詳細図を示す。

【 0 0 2 6 】

フローチャートは実施の形態 1 で説明した図 6、図 7 と同様であるが（ただし図 6 のデスクランブル処理部での処理（S 7 0 5）はデスクランブル処理部とセキュリティモジュールでの処理になる）、図 7 のステップ S 8 0 3 はセキュリティモジュール内での処理になる。また、ステップ S 8 0 3 において、スクランブル鍵をセキュリティモジュール 3 0 0 からデスクランブル部へ渡す時には暗号をかけ、受信機での処理が終了後はすぐに受信機内のメモリ上からスクランブル鍵を削除すればよい。

【 0 0 2 7 】

（実施の形態 3）

次に、TS パケットとスクランブルキーの対応をECMへの記述と、TS パケットの非スクランブル部とを利用する方法について説明する。ここでの方法によれば、図9のデータ構造中TS_packet_numberが不要になるため、伝送容量の節約にもなる。

【0028】

以下、TS パケットの非スクランブル部の中のCC (Continuity Counter) を利用する方法について説明する。CCとはTS パケットヘッダーの4ビットを使用した巡回カウンタ(値0から1ずつ増加して15までいったら0に戻る)で、同じパケットIDを持つTS パケットが途中で一部破棄されたかどうかを検出するための情報であり、国際標準規格MPEG2システムで規定されている。

【0029】

本発明の実施の形態3によるシステム全体の構成は、実施の形態1による構成である図1と同様であるが、その中のスクランブル処理部103とデスクランブル処理部204の構成が異なるので、図15にスクランブル処理部103の構成を図16にデスクランブル処理部の構成を示す。

【0030】

スクランブル処理部103は、スクランブル鍵識別子算出部120と、TS パケットヘッダ解釈部121と、スクランブル鍵リスト保持部122と、スクランブル部123と、スクランブル鍵リスト解釈部124からなる。

【0031】

デスクランブル処理部204は、TS パケット抽出部220と、スクランブル鍵識別子算出部221と、デスクランブル部222と、スクランブル鍵リスト解釈部223からなる。

【0032】

(放送装置側)

放送装置100において映像、音声、データなどのコンテンツにスクランブルをかける際の動作手順を示すフローチャートは図4と同様であるが、スクランブル処理部103における処理(ステップS505)が異なるので、図17にその

フローチャートを示す。図 1 と図 1 5 も用いて説明する。

【 0 0 3 3 】

スクランブル鍵リスト生成部 1 0 2 から、スクランブル鍵リストを取得し、スクランブル鍵リスト保持部 1 2 2 に格納する（ステップ S 9 0 1）。TS パケット化処理部 1 0 1 で TS パケット化された（ステップ S 5 0 4）コンテンツを TS パケットヘッダ解釈部 1 2 1 において、1 TS パケット分取得する（ステップ S 9 0 2）。1 TS パケット分取得した時に TS パケットヘッダ解釈部 1 2 1 は、CC の値を読み取り、読み取った CC の値をスクランブル鍵識別子算出部 1 2 0 へ渡し、TS パケットをスクランブル部 1 2 3 へ渡す（ステップ S 9 0 3）。スクランブル鍵識別子算出部 1 2 0 において、CC の値からスクランブル鍵識別子を算出し、スクランブル鍵リスト解釈部 1 2 4 へ渡す（ステップ S 9 0 4）。スクランブル鍵リスト解釈部 1 2 4 においてスクランブル鍵識別子とスクランブル鍵リスト保持部 1 2 2 に格納してあるスクランブル鍵リストから該当スクランブル鍵を抽出して、スクランブル部 1 2 3 へ渡す（ステップ S 9 0 5）。スクランブル部 1 2 3 において、ステップ S 9 0 3 で取得した 1 TS パケット分を、ステップ S 9 0 5 で取得したスクランブル鍵でスクランブルをかけ、多重化処理部 1 0 6 へ渡し（ステップ S 9 0 6）、全 TS パケット分取得したかどうかを判定して（ステップ S 9 0 7）、取得完了していれば処理を終了し、そうでなければ、ステップ S 9 0 2 からの処理を繰り返す。ステップ S 9 0 4 における CC の値からスクランブル鍵識別子を算出する方法には、例えば、 $CC \bmod n$ （ $1 \leq n \leq 16$ ）（なお、 \bmod とは、CC を n で割った余りである）の値をスクランブル鍵識別子とする方法がある。この算出方法によれば、CC の値は 0 から 15 までの値をとるために、 $n = 16$ の場合、スクランブル鍵リストは図 20 に示すように、識別子 0 から 15 までの 16 個のスクランブル鍵から構成される。例えば CC の値が 2 の TS パケットは、2 を 16 で割った余りが 2 なので識別子の値は 2 となり、スクランブル鍵 $K_s 3$ を使ってスクランブルする。なお、スクランブル鍵を CC の値から算出する方法にすることにより、CC の値をそのままスクランブル鍵識別子とするより、スクランブル鍵識別子の値が見破られることを防止できる。

【 0 0 3 4 】

n の値を 1 6 として説明したが、1 から 1 5 までの値でもかまわない。n の値を変更することによって、スクランブル鍵リストを作成した後で、再度作成し直すことなく使用するスクランブル鍵の数を容易に変更できる。例えば、図 2 0 に示すようなスクランブル鍵リストを変更せずに、n の値を 4 に変更することにより、識別子の値は 0 から 3 までとなり、使用するスクランブル鍵は K s 1、K s 2、K s 3、K s 4 の 4 つとなる。なお、n の値は算出方法として、予め固定値としてもよい、図 8 に示した蓄積用 E C M の可変部に記述してもよい。

【 0 0 3 5 】

また、C C の値を利用するのではなく、C C と同様に国際標準規格 M P E G 2 システムで規定されているプログラム時刻基準参照値である P C R (P r o g r a m C l o c k R e f e r e n c e)、またはオリジナルプログラム時刻基準参照値である O P C R (O r i g i n a l P C R) の特定のビット（例えば、4 ビットにすれば C C と全く同様に処理することができる）を利用してもかまわない。

【 0 0 3 6 】

また、既に使用方法が M P E G 2 システムで規定されている領域を利用するのではなく、アダプテーション・フィールド部のプライベートデータ領域のようにユーザが自由に使用できる領域に、スクランブル鍵識別子の値を直接記述してもよい。

【 0 0 3 7 】

(受信機側)

T S 分離部 2 0 1 で蓄積用 E C M とスクランブルコンテンツを分離して H D D 2 0 2 に蓄積後に、受信機 2 0 0 でスクランブルコンテンツをデスクランブルする際の動作手順を示すフローチャートは図 6 と同様であるが、デスクランブル処理部 2 0 4 における処理（ステップ S 7 0 5）が異なるので、図 1 8 にそのフローチャートを示す。図 1 と図 1 6 も用いて説明する。なお、蓄積用 E C M とスクランブルコンテンツを分離せずに一つの T S として蓄積してもよい。

【 0 0 3 8 】

ステップ S 7 0 4 で渡されたスクランブルコンテンツを T S パケット抽出部 2 2 0 において、1 T S パケット分抽出する（ステップ S 1 0 0 1）。1 T S パケット分抽出した時に T S パケット抽出部 2 2 0 は、当該 T S パケットの C C の値を読み取り、読み取った C C の値を、スクランブル鍵識別子算出部 2 2 1 へ渡し、抽出した T S パケットをデスクランブル部 2 2 2 へ渡す（ステップ S 1 0 0 2）。スクランブル鍵識別子算出部 2 2 1 において、C C の値からスクランブル鍵識別子を算出し、スクランブル鍵リスト解釈部 2 2 3 へ渡す（ステップ S 1 0 0 3）。スクランブル鍵リスト解釈部 2 2 3 においてスクランブル鍵識別子とスクランブル鍵リスト保持部 2 0 3 に格納してあるスクランブル鍵リストから該当スクランブル鍵を抽出して、デスクランブル部 2 2 2 へ渡す（ステップ S 1 0 0 4）。デスクランブル部 2 2 2 において、ステップ S 1 0 0 2 で取得した 1 T S パケット分を、ステップ S 1 0 0 4 で取得したスクランブル鍵でデスクランブルし、再生処理部へ渡す（ステップ S 1 0 0 5）。全 T S パケット分取得したかどうかを判定して（ステップ S 1 0 0 6）、取得完了していれば処理を終了し、そうでなければ、ステップ S 1 0 0 1 からの処理を繰り返す。

【 0 0 3 9 】

ステップ S 1 0 0 3 における C C の値からスクランブル鍵識別子を算出する方法は、前述の放送装置で説明した方法と同じである。

【 0 0 4 0 】

【発明の効果】

本発明では、スクランブル鍵リストを送出することによって、蓄積後のスクランブルコンテンツを再生する場合に、再生対象となる任意の T S パケットに対応するスクランブル鍵を、スクランブル鍵リストから即座に抽出することができる。

【 0 0 4 1 】

スクランブル鍵リストの送出周期は長周期にすることができるので、伝送容量の節約ならびに、送出装置の送出タイミング制御処理を軽減することが容易である。

【 0 0 4 2 】

また、一つのコンテンツに対して複数のスクランブル鍵を使用することによって従来通りのセキュリティ強度も保証できる。

【 0 0 4 3 】

さらに、スクランブル鍵リストをセキュリティモジュール内に格納することにより、スクランブル鍵リストが悪質なユーザによって見破られることを防止することができる。

【 0 0 4 4 】

以上のように、スクランブルコンテンツを蓄積し、蓄積後の特殊再生機能を、ユーザの満足できる性能で、またセキュリティ強度も保証した方法で実現できる。

【図面の簡単な説明】

【図 1】

システムの全体構成図

【図 2】

本発明の実施の形態 1 におけるスクランブル処理部の構成図

【図 3】

本発明の実施の形態 1 におけるデスクランブル処理部の構成図

【図 4】

本発明の実施の形態 1 における放送装置の動作手順を示すフローチャート

【図 5】

本発明の実施の形態 1 におけるスクランブル処理部の動作手順を示すフローチャート

【図 6】

本発明の実施の形態 1 における受信機の動作手順を示すフローチャート

【図 7】

本発明の実施の形態 1 におけるデスクランブル処理部の動作手順を示すフローチャート

【図 8】

蓄積用 ECM のデータ構造の例を示す図

【図 9】

スクランブル鍵リスト記述子のデータ構造の例を示す図

【図 1 0】

フローチャートの補足説明する具体例を示す図

【図 1 1】

スクランブル鍵リストの具体例を示す第一の図

【図 1 2】

早送り再生機能を説明するための具体例を示す図

【図 1 3】

本発明の実施の形態 2 における受信機の構成図

【図 1 4】

本発明の実施の形態 2 におけるデスクランブル処理部の構成図

【図 1 5】

本発明の実施の形態 3 におけるスクランブル処理部の構成図

【図 1 6】

本発明の実施の形態 3 におけるデスクランブル処理部の構成図

【図 1 7】

本発明の実施の形態 3 におけるスクランブル処理部の動作手順を示すフローチャート

【図 1 8】

本発明の実施の形態 3 におけるデスクランブル処理部の動作手順を示すフローチャート

【図 1 9】

スクランブル鍵リストの送出タイミングを示す図

【図 2 0】

スクランブル鍵リストの具体例を示す第 2 の図

【図 2 1】

MPEG2 符号化方式による映像ストリームの概念図

【図 2 2】

本発明の実施の形態 1 における早送り再生時のデスクランブル処理部の動作手順を示すフローチャート

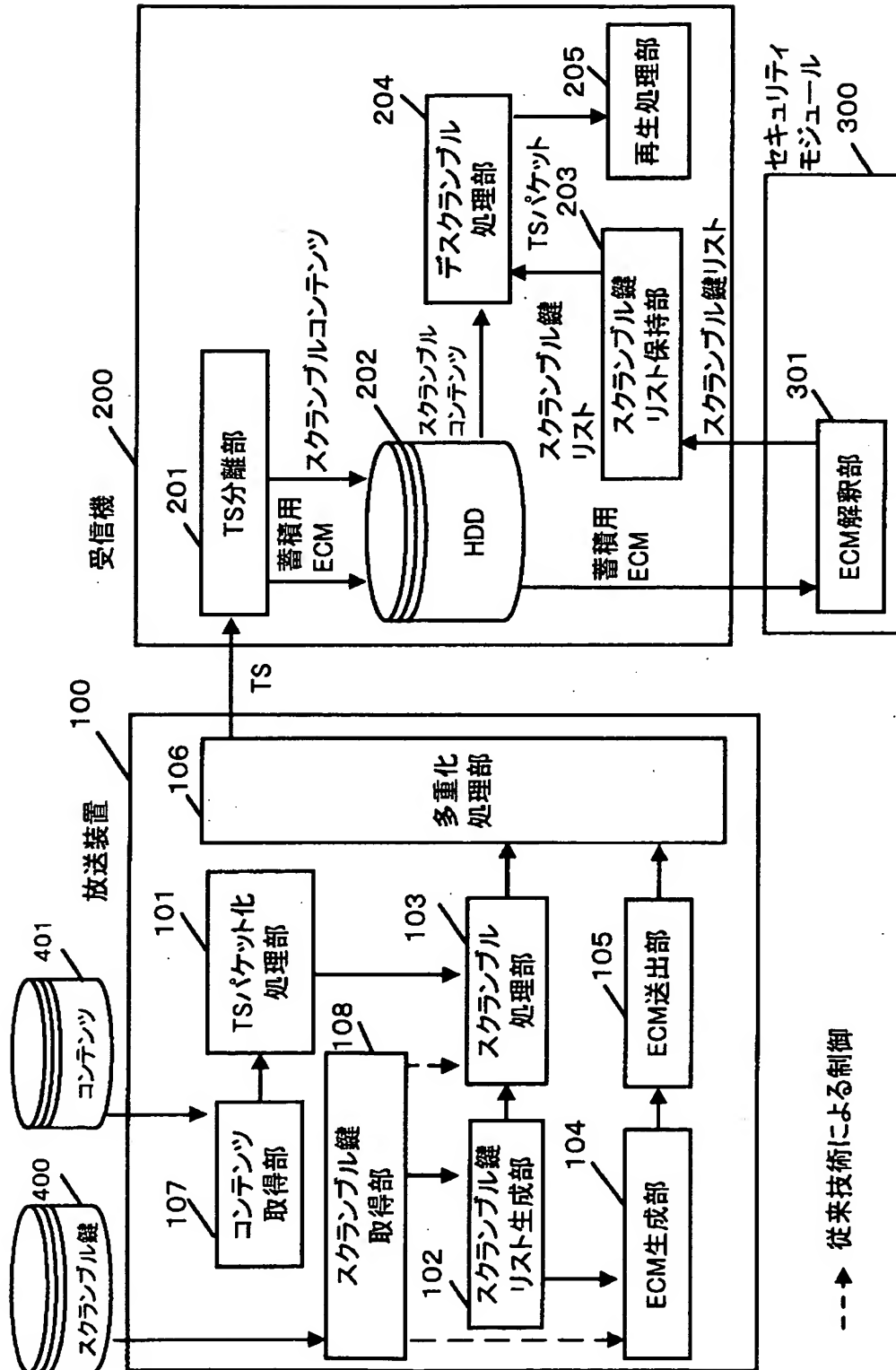
【符号の説明】

- 1 0 0 放送装置
- 1 0 1 TS パケット化処理部
- 1 0 2 スクランブル鍵リスト生成部
- 1 0 3 スクランブル処理部
- 1 0 4 ECM 生成部
- 1 0 5 ECM 送出部
- 1 0 6 多重化処理部
- 1 0 7 コンテンツ取得部
- 1 0 8 スクランブル鍵取得部
- 1 1 0 TS パケットカウンタ部
- 1 1 1, 1 2 2, 2 0 3 スクランブル鍵リスト保持部
- 1 1 2, 1 2 3 スクランブル部
- 1 1 3, 1 2 4, 2 1 2, 2 2 3 スクランブル鍵リスト解釈部
- 1 2 0, 2 2 1 スクランブル鍵識別子算出部
- 1 2 1 TS パケットヘッダ解釈部
- 2 0 0 受信機
- 2 0 1 TS 分離部
- 2 0 2 HDD
- 2 0 4 デスクランブル処理部
- 2 0 5 再生処理部
- 2 1 0, 2 2 0 TS パケット抽出部
- 2 1 1, 2 2 2 デスクランブル部
- 3 0 0 セキュリティモジュール
- 3 0 1 ECM 解釈部
- 4 0 0 スクランブル鍵
- 4 0 1 コンテンツ

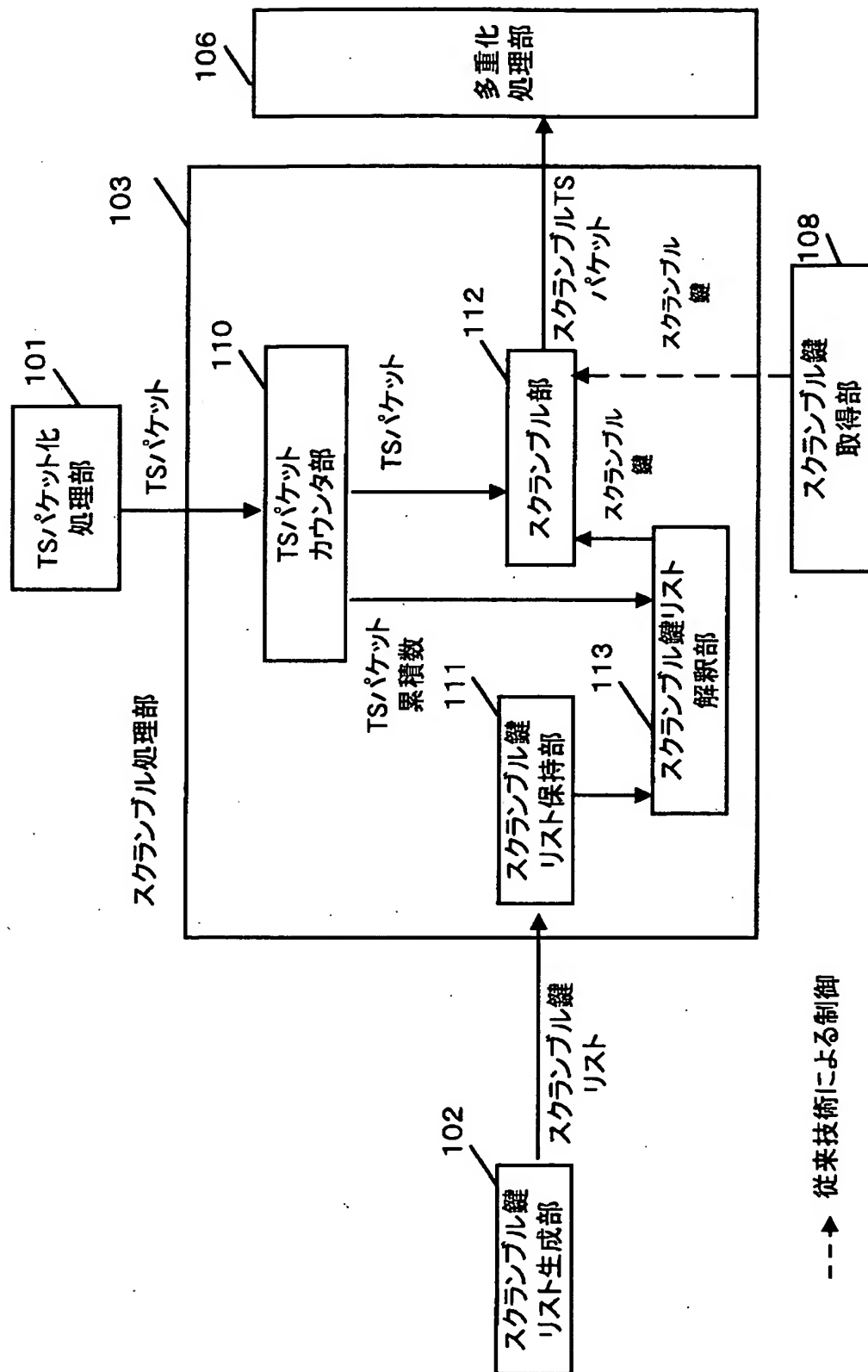
【書類名】

凶面

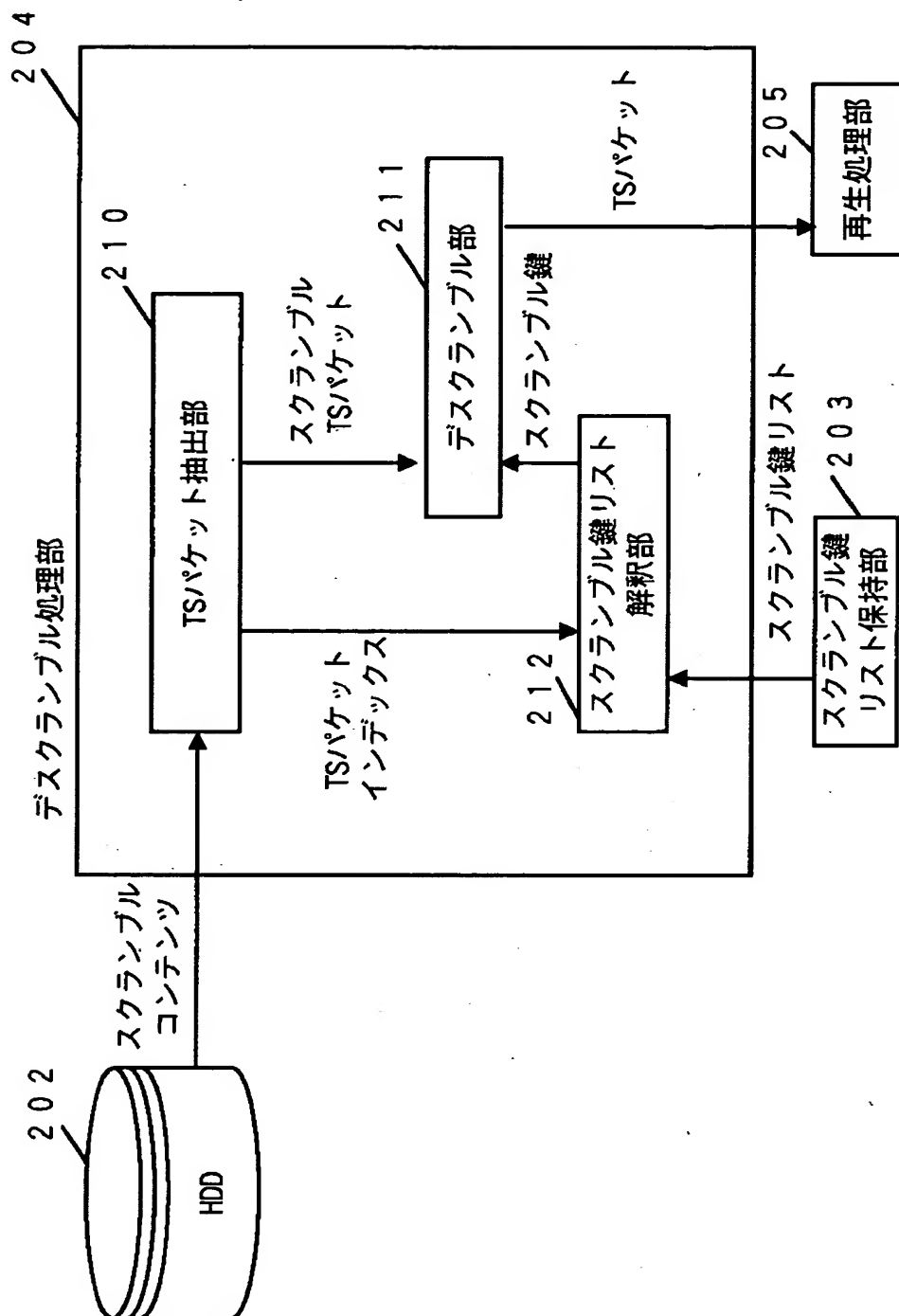
【図 1】



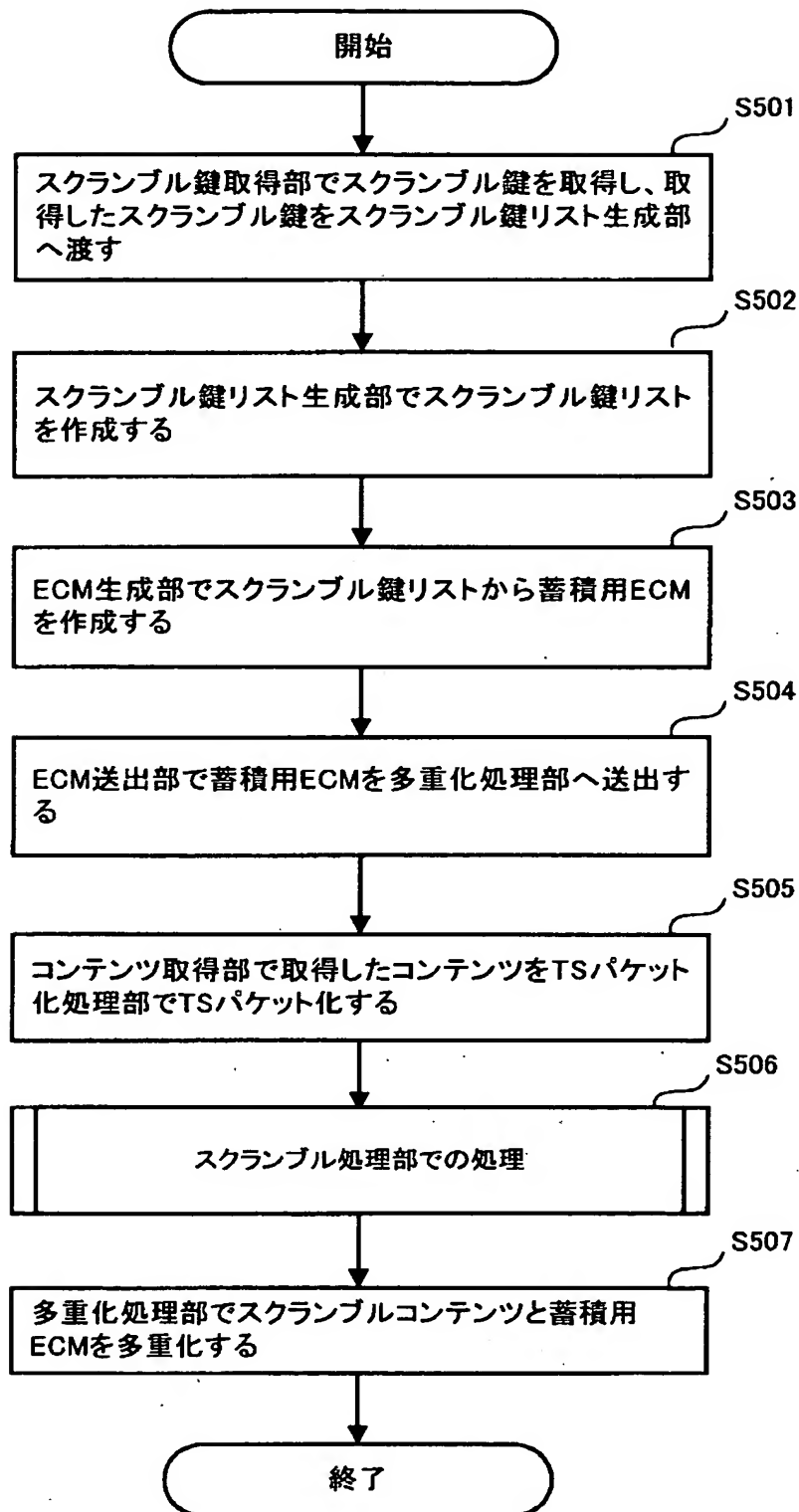
【図 2】



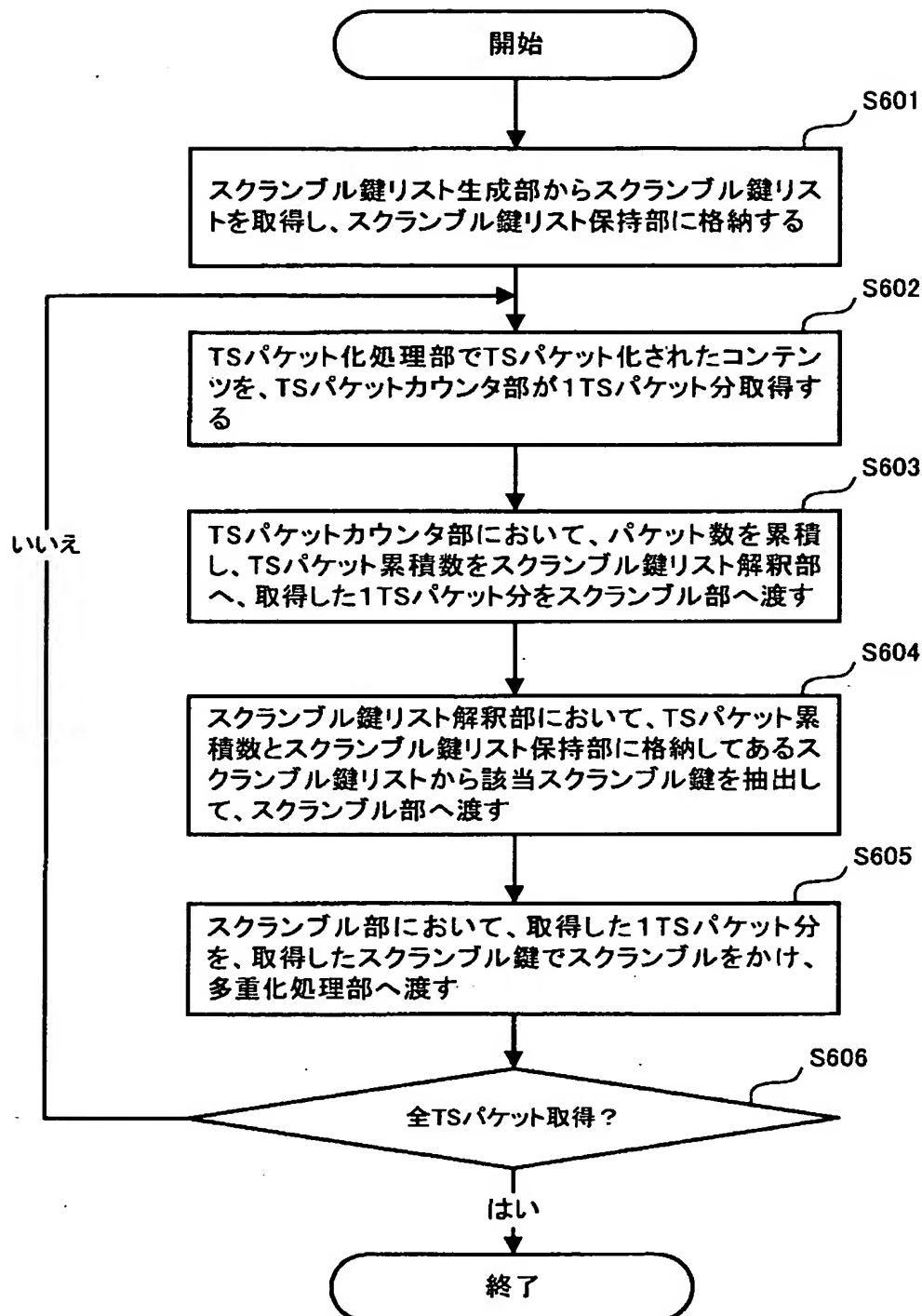
【図 3】



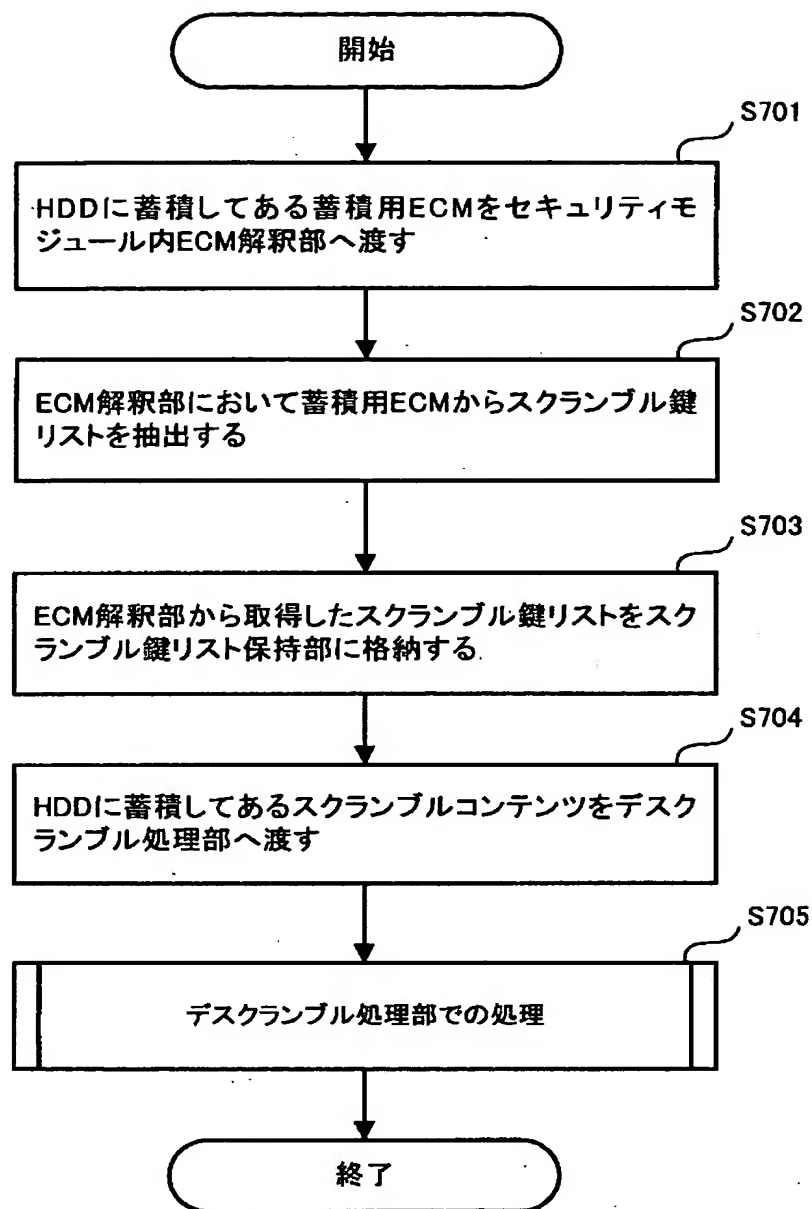
【図 4】



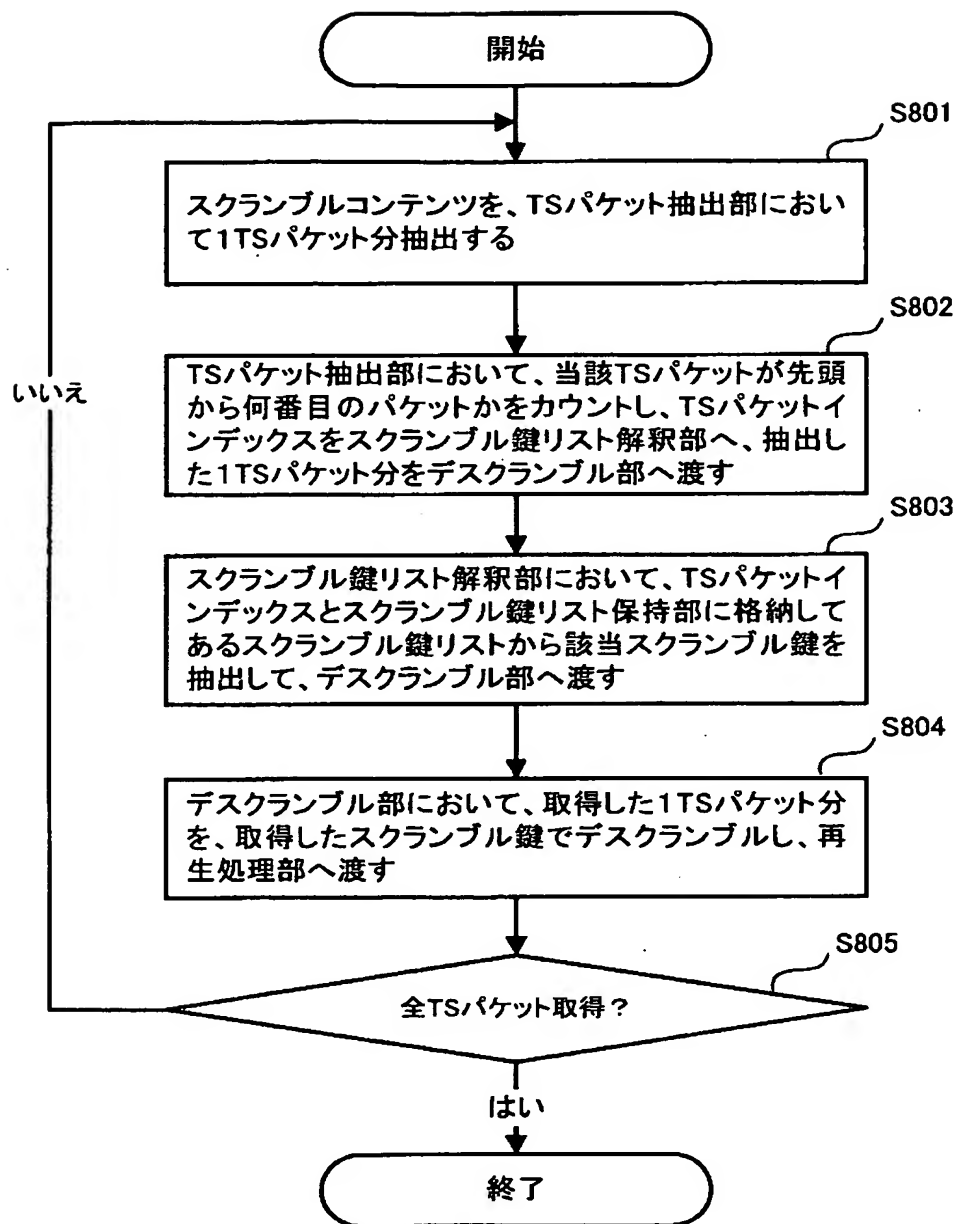
【図 5】



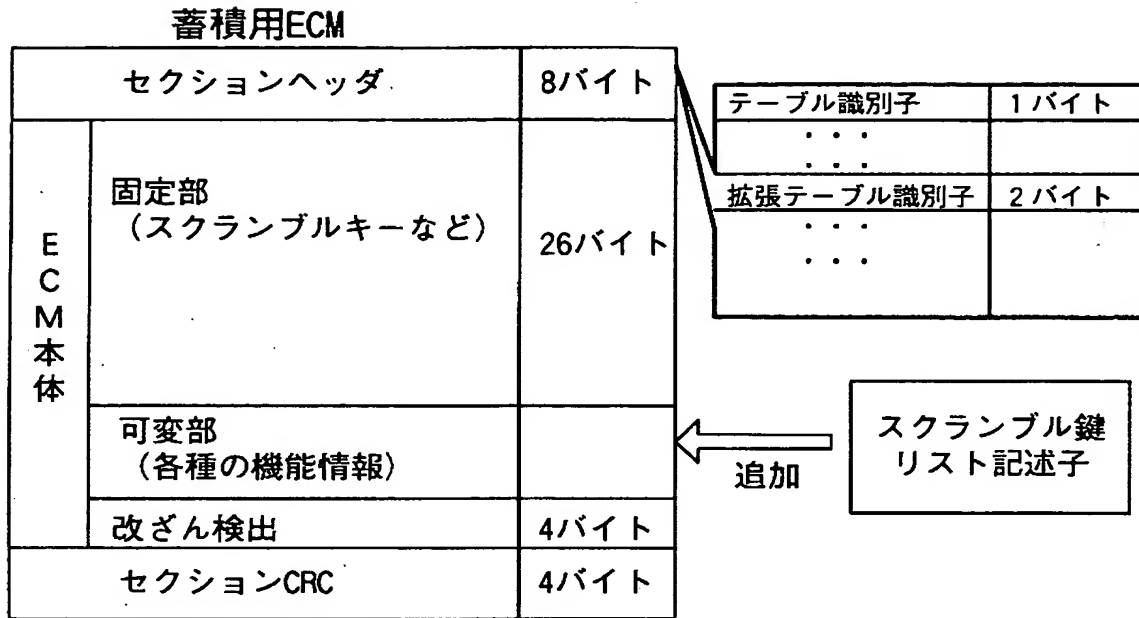
【図 6】



【図 7】



【図 8】



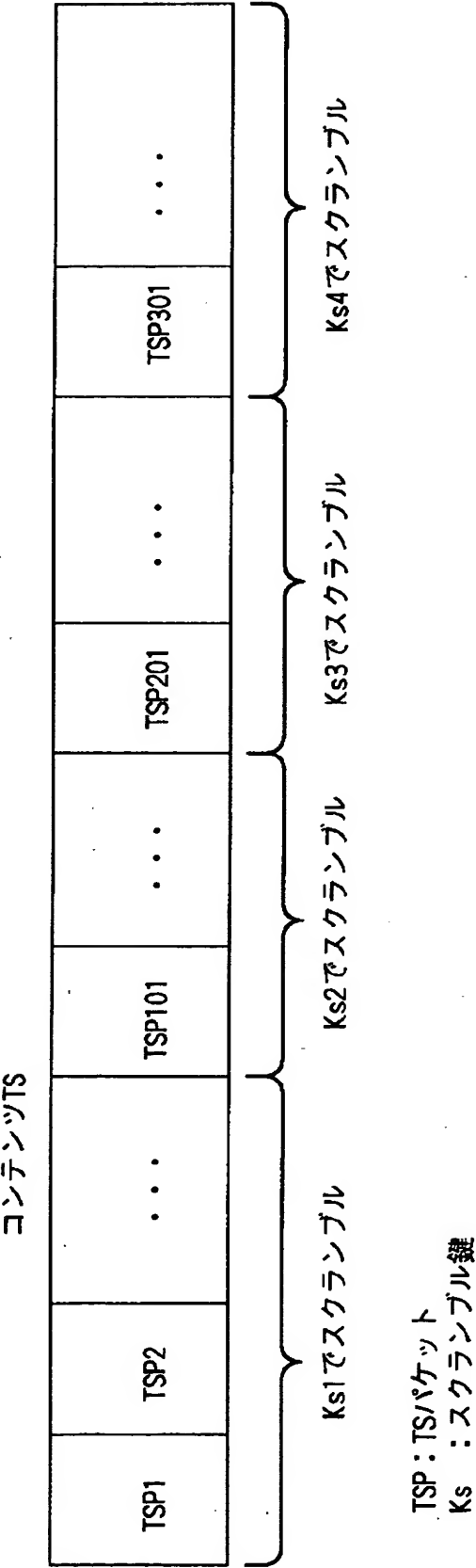
【図 9】

スクランブル鍵リスト記述子のデータ構造

<pre> CA_Ks_List_descriptor() { descriptor_tag descriptor_length for(i=0; i<N; i++) { Ks_id TS_packet_number Ks } } </pre>	1バイト 1バイト 1バイト 2バイト 8バイト
---	--

Ks_id : スクランブル鍵識別子 (スクランブル鍵の識別をする)
 TS_packet_number : 当該KsでスクランブルしているTSパケット数
 Ks : スクランブル鍵

【図 1 0】

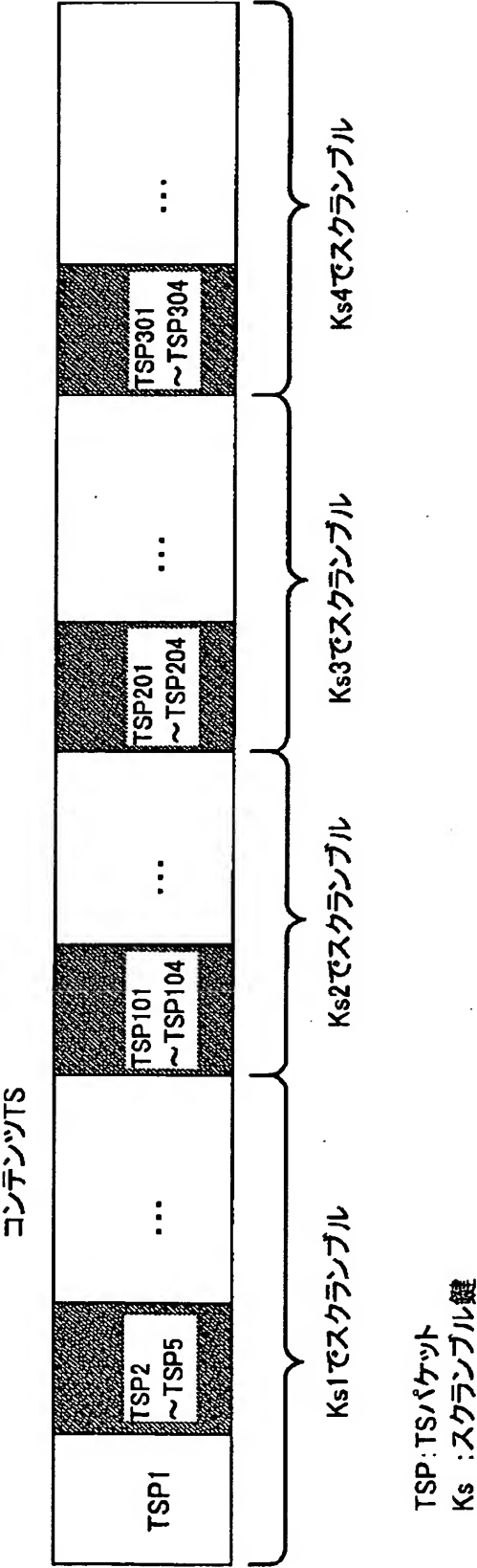


【図 1 1】

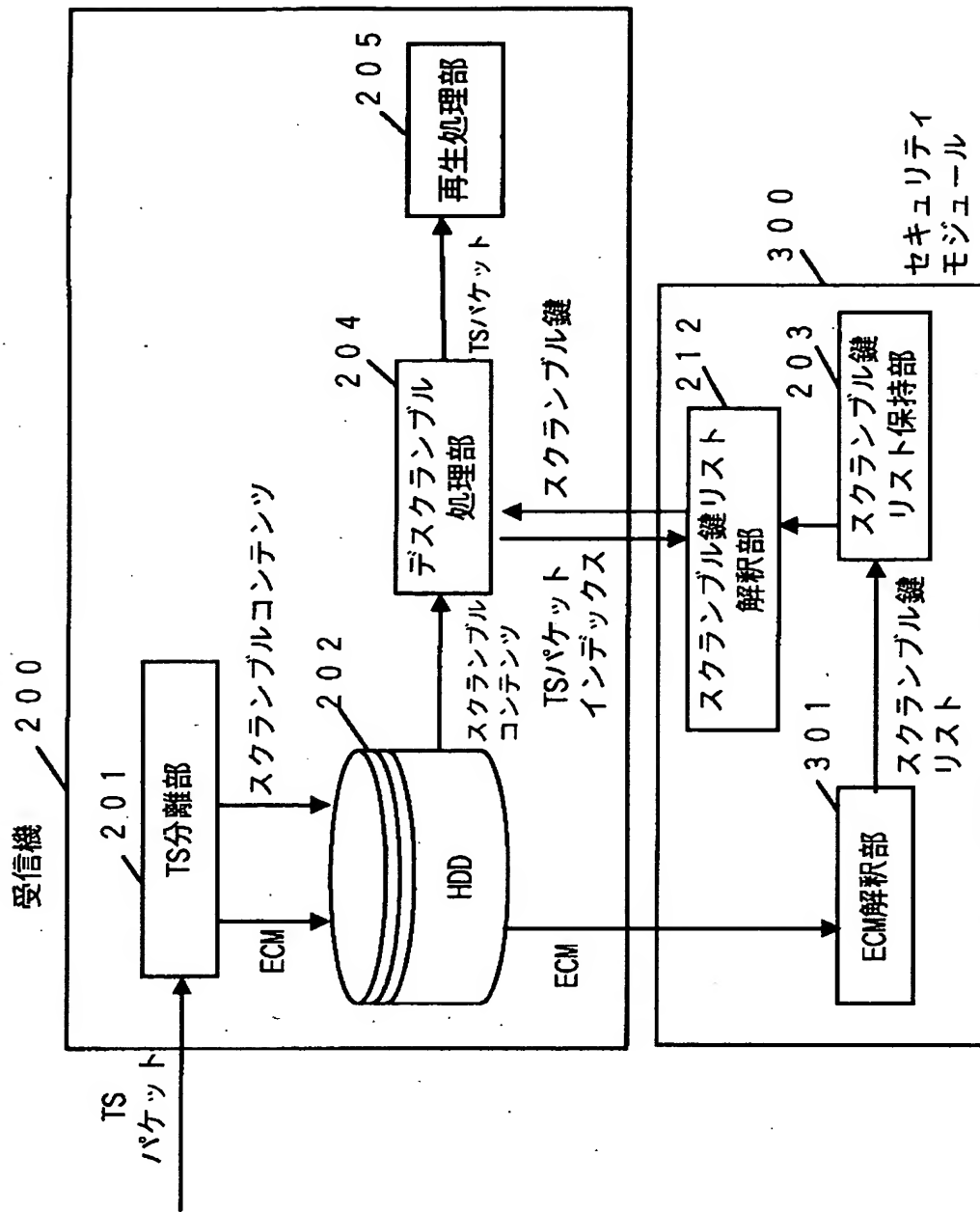
スクランブル鍵リスト

Ks_id	1
TS_packet_number	1 0 0
Ks	K s 1
Ks_id	2
TS_packet_number	1 0 0
Ks	K s 2
Ks_id	3
TS_packet_number	1 0 0
Ks	K s 3
Ks_id	4
TS_packet_number	1 0 0
Ks	K s 4

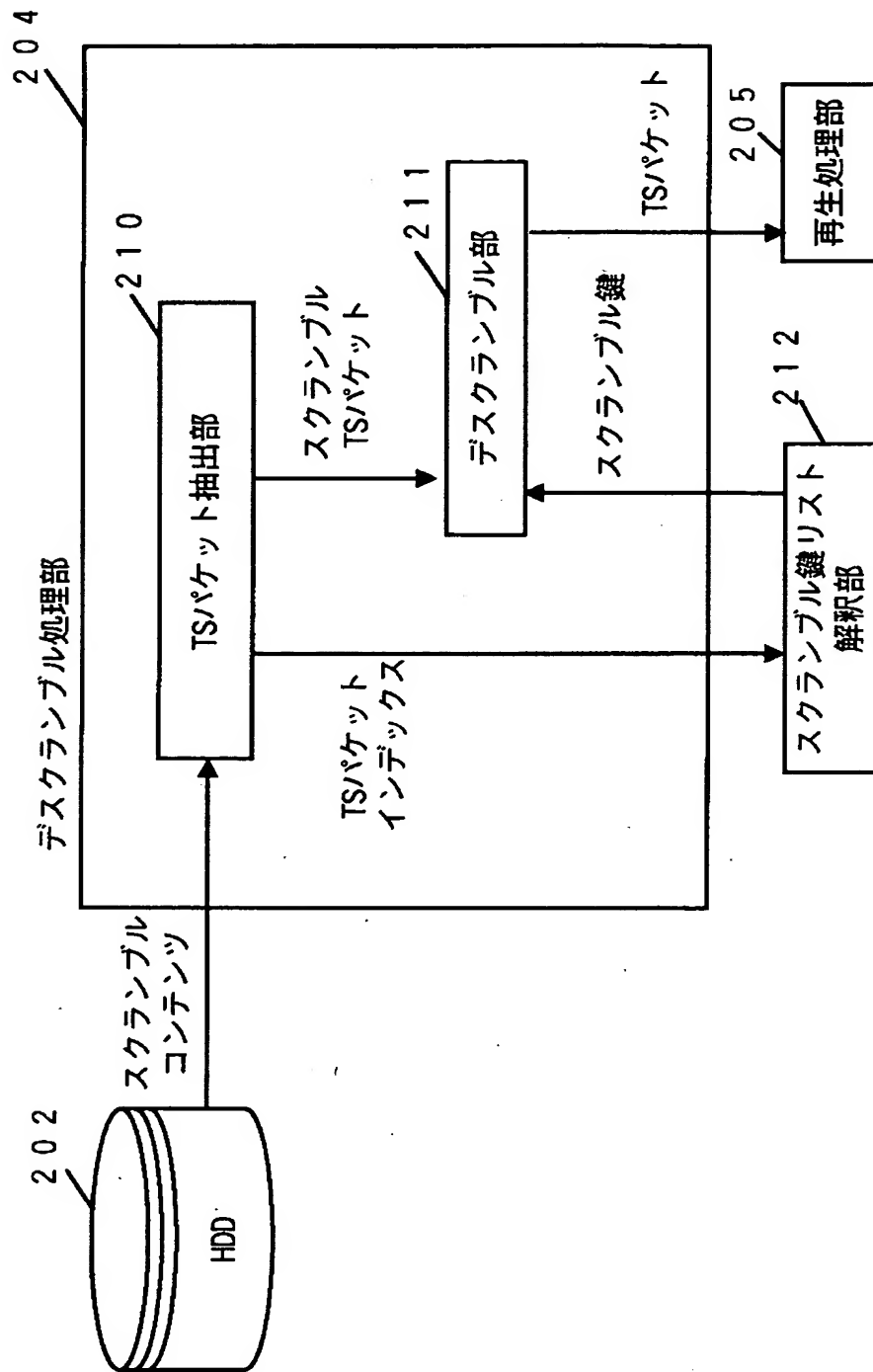
【図 1 2】



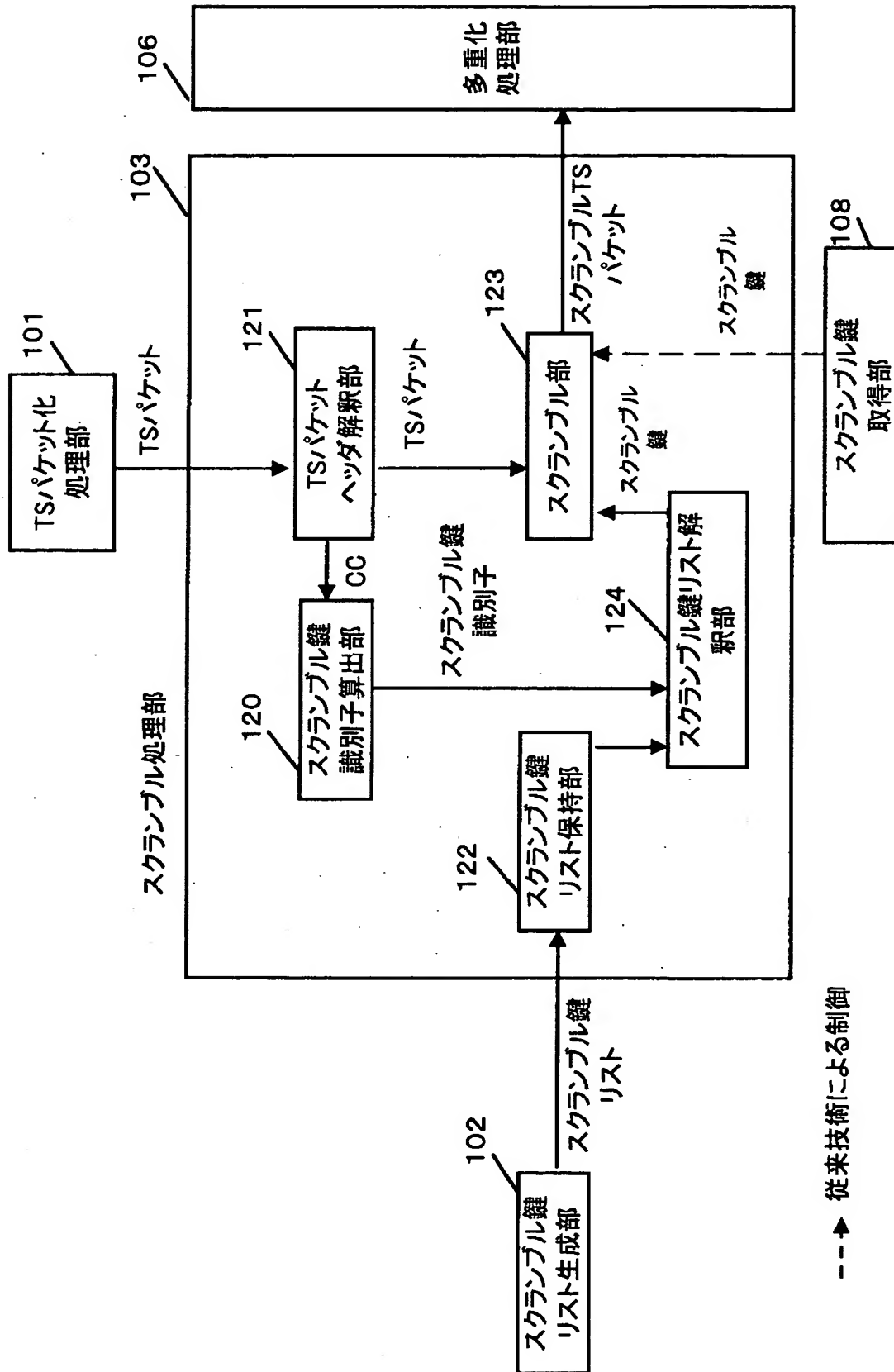
【図13】



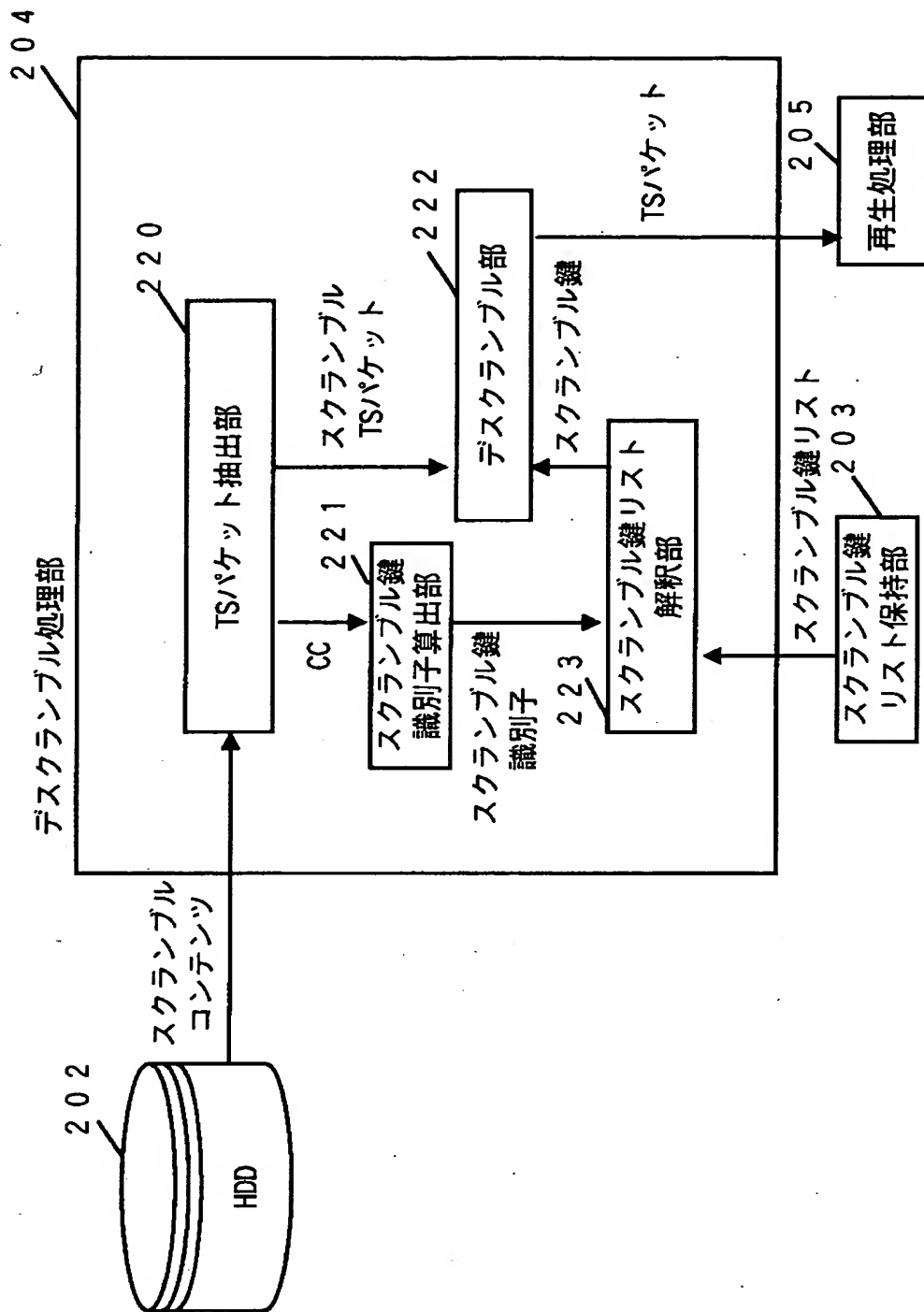
【図 1 4】



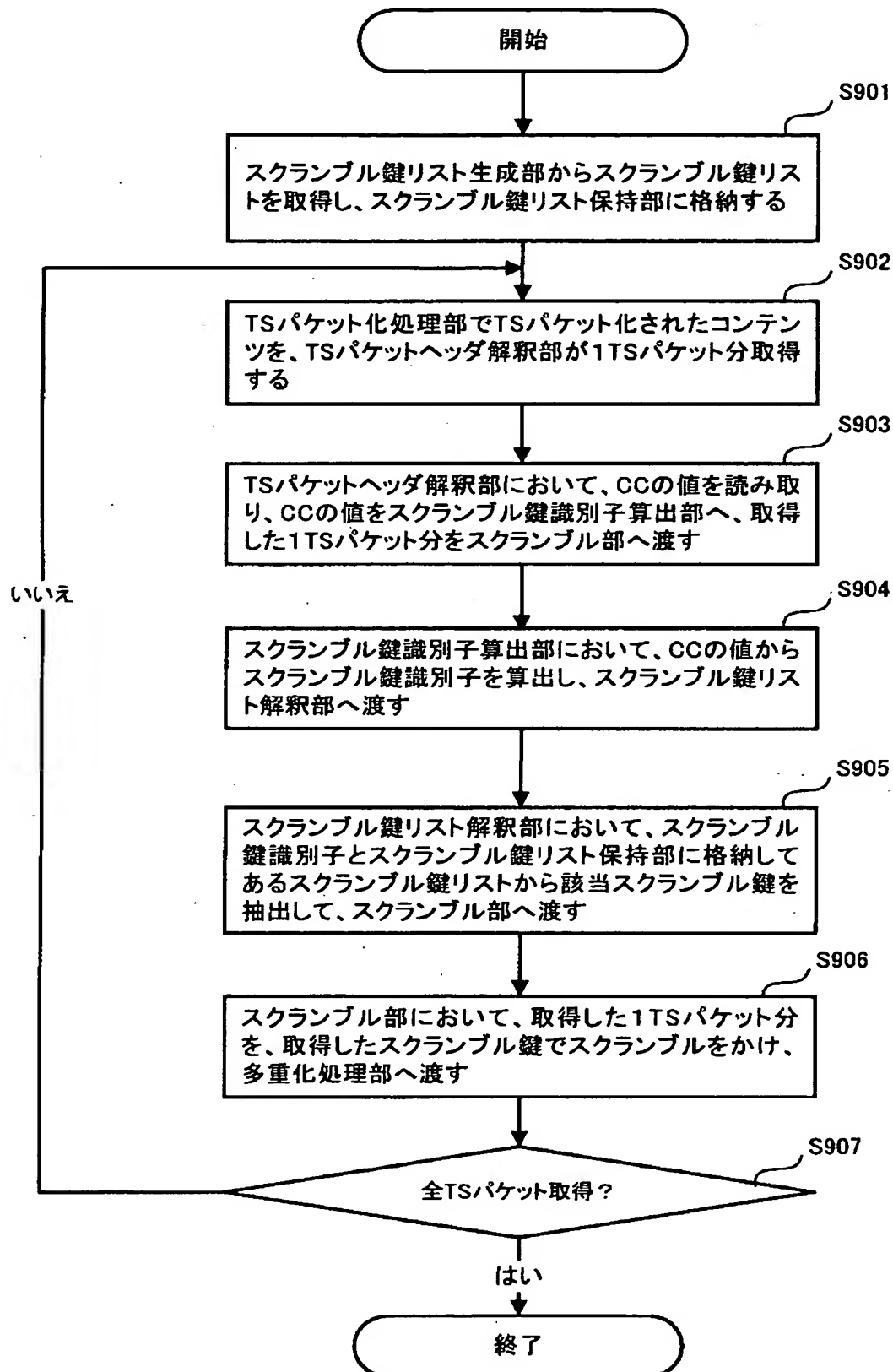
【図 15】



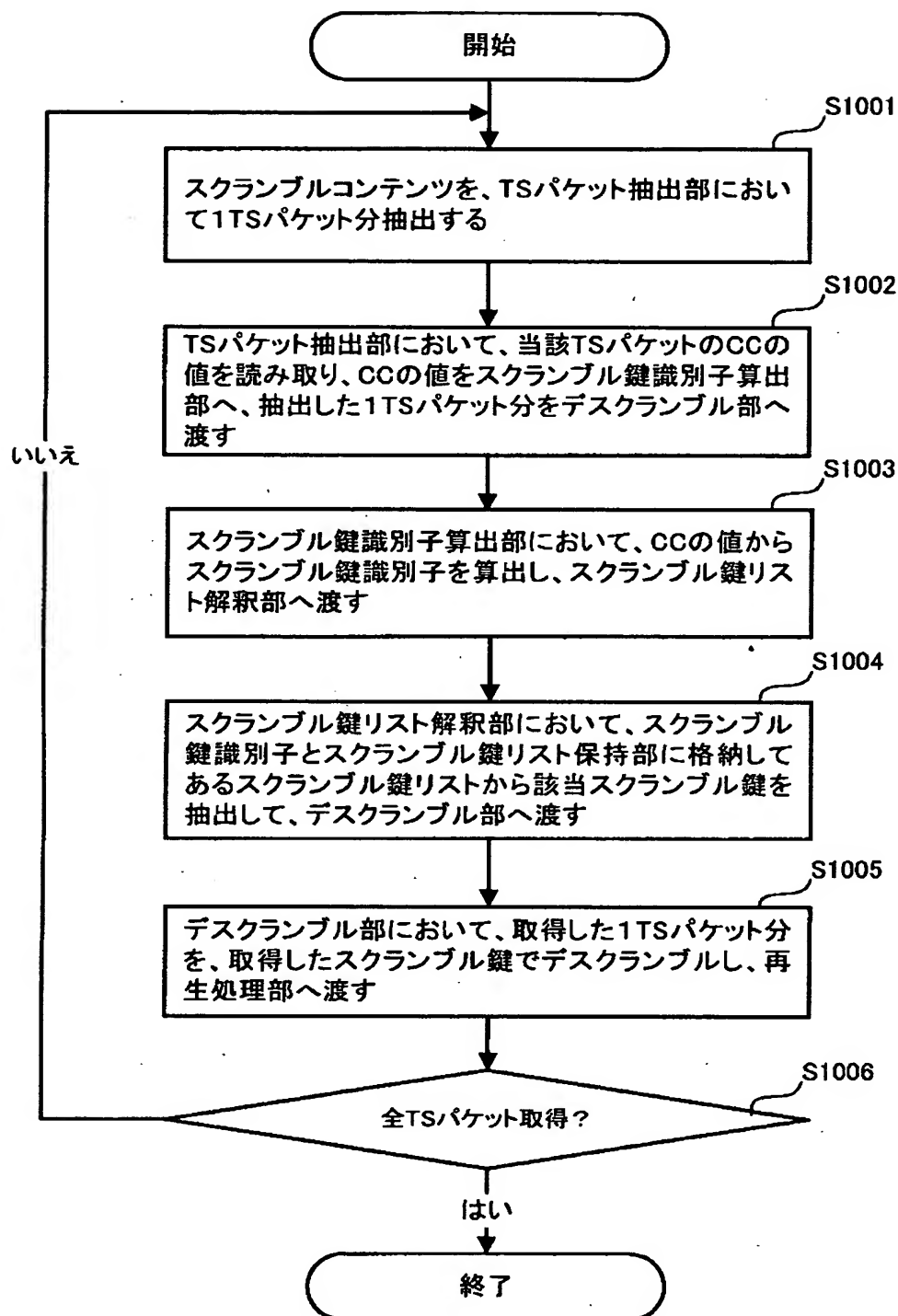
【図16】



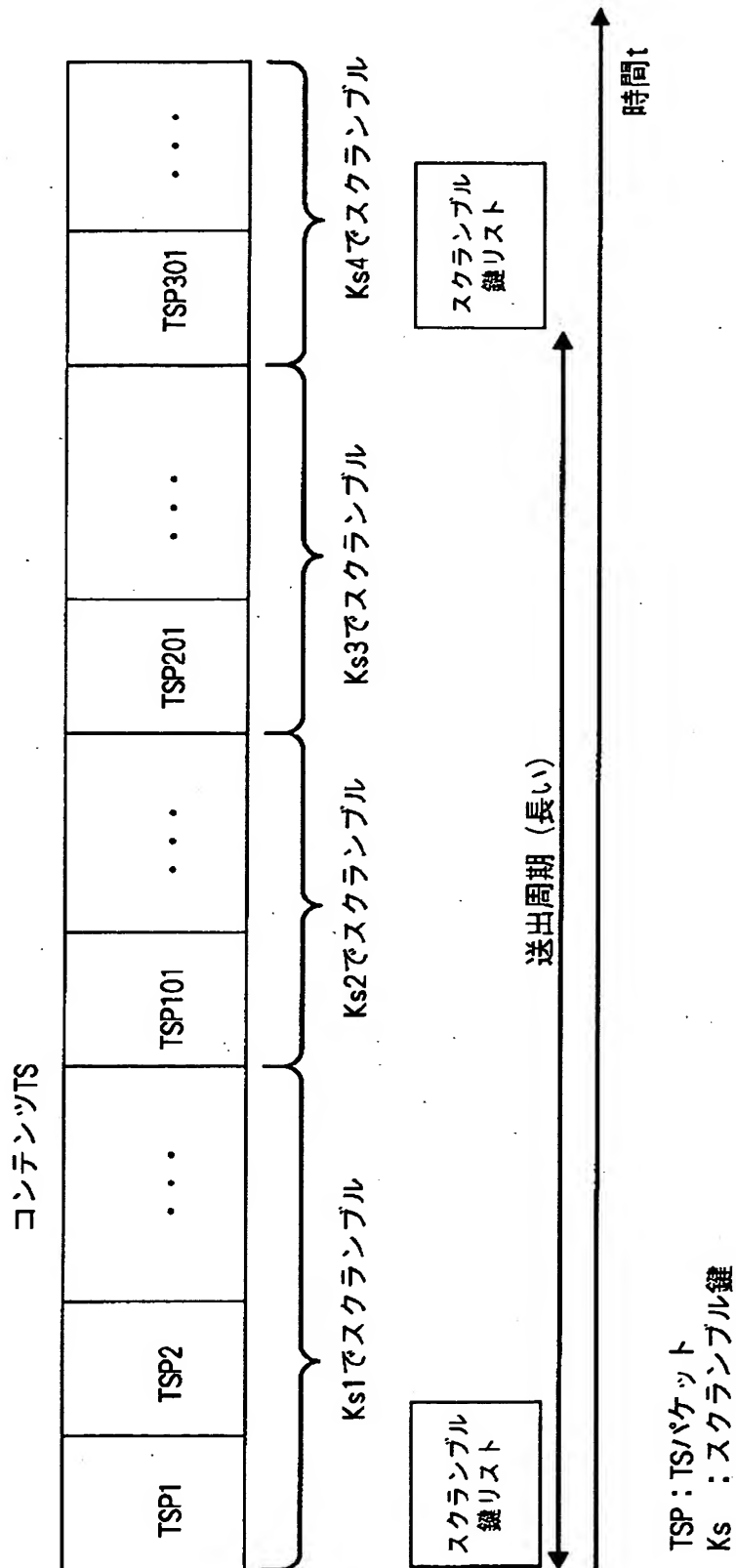
【図 17】



【図 1 8】



【図19】

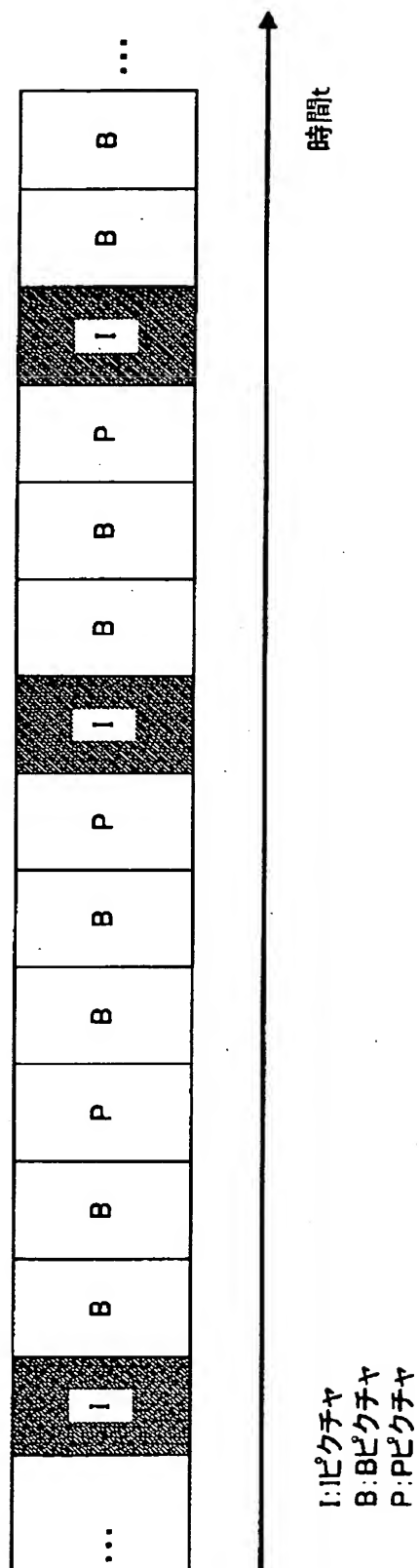


【図 2 0】

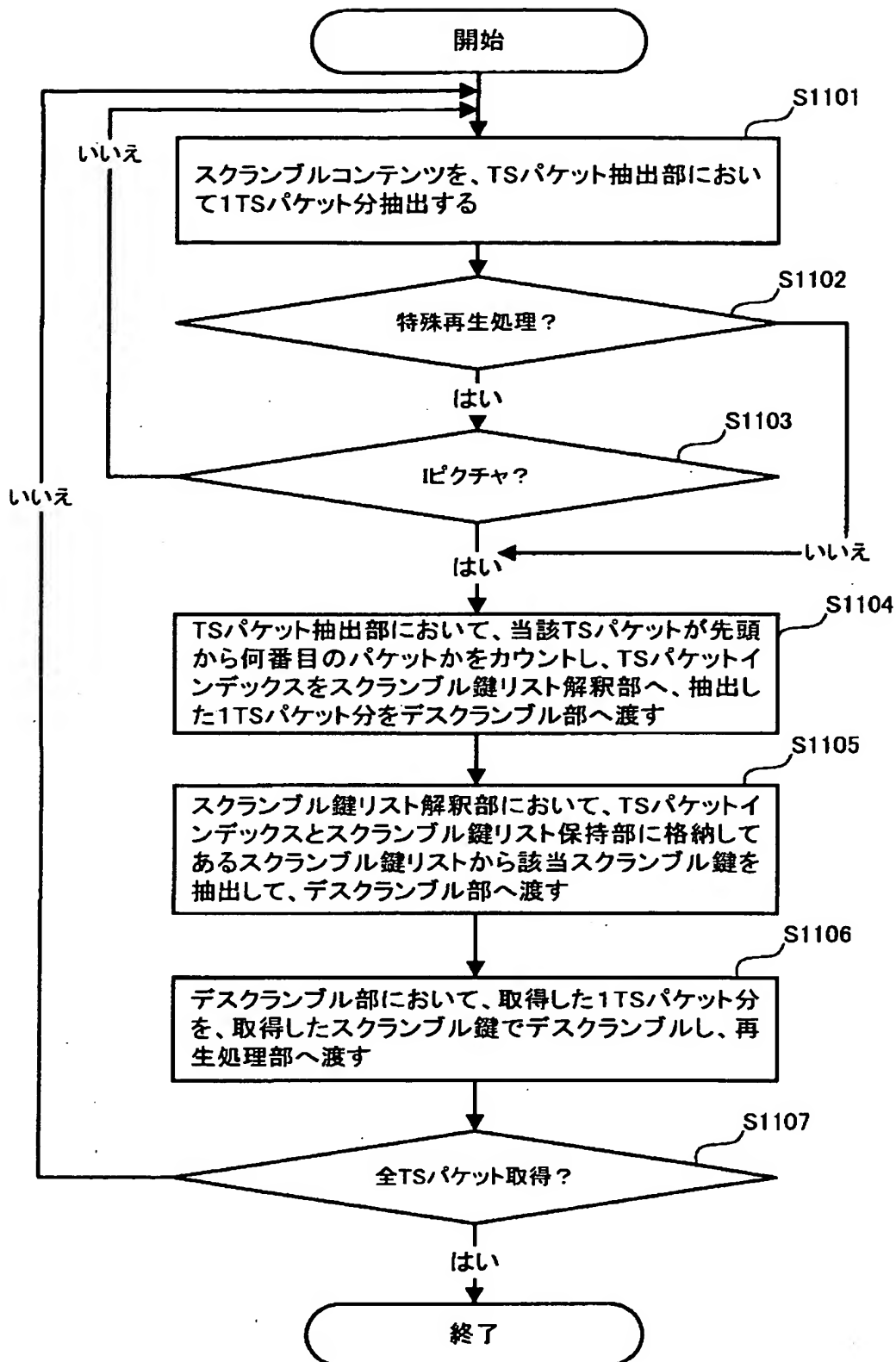
スクランブル鍵リスト

Ks_id	0
Ks	Ks1
Ks_id	1
Ks	Ks2
Ks_id	2
Ks	Ks3
Ks_id	3
Ks	Ks4
Ks_id	4
Ks	Ks5
Ks_id	5
Ks	Ks6
Ks_id	6
Ks	Ks7
Ks_id	7
Ks	Ks8
Ks_id	8
Ks	Ks9
Ks_id	9
Ks	Ks10
Ks_id	10
Ks	Ks11
Ks_id	11
Ks	Ks12
Ks_id	12
Ks	Ks13
Ks_id	13
Ks	Ks14
Ks_id	14
Ks	Ks15
Ks_id	15
Ks	Ks16

【図 2 1】



【図 22】



【書類名】 要約書

【要約】

【課題】 スクランブルコンテンツを蓄積し、蓄積後の特殊再生機能を、ユーザの満足できる性能で実現する。

【解決手段】 放送装置は、スクランブル鍵のリストを作成するスクランブル鍵リスト生成手段と、前記スクランブル鍵リストから蓄積用 E C M を作成する E C M 生成手段と、前記蓄積用 E C M を送出する E C M 送出手段と、 T S パケット単位でスクランブルをかけるスクランブル処理手段を備え、受信機は、受信した蓄積用 E C M からスクランブル鍵リストを抽出する E C M 解釈手段と、スクランブル鍵リストから該当 T S パケットのスクランブル鍵を抽出するスクランブル鍵リスト解釈手段と、 T S パケット単位でデスクランブルするデスクランブル処理手段とを備える。

【選択図】 図 1

出 願 人 履 歴 情 報

識別番号 [000005821]

1. 変更年月日 1990年 8月28日

[変更理由] 新規登録

住 所 大阪府門真市大字門真1006番地

氏 名 松下電器産業株式会社